

Editor's Comments*

Welcome to the second issue of *The Journal of Physical Security* (JPS). Just a few random thoughts and comments:

1. If you haven't already read John Mueller's book, *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them*, it is definitely worth a look. The author presents a provocative argument that our current homeland security response to terrorism is totally out of whack with the true threat, and is often misdirected and wasteful.

2. If you want to read something interesting, fun, and frightening simultaneously, check out these two books on drug counterfeiting: Katherine Eban, *Dangerous Doses: How Counterfeiters Are Contaminating America's Drug Supply* and Tim Phillips, *Knockoff: The Deadly Trade in Counterfeit Goods: The True Story of the World's Fastest Growing Crime Wave*. Counterfeiting (and tampering) with pharmaceuticals and other consumer products is going to be a huge issue in the coming years.

3. CSO ran an interesting article in August of 2006 entitled, *"Don't Shoot the Messenger: The first security assessment at my new employer wasn't supposed to be personal. It just ended up that way."* This is really about cyber security, but the issues discussed are probably even more relevant for physical security. See: http://www.csoonline.com/read/080106/col_undercover.html By the way CSO (Chief Security Officer) Magazine continues to be one of the more thoughtful security trade journals, and often covers physical security concerns. Almost every issue has one or more articles that are quite fascinating. Plus it's free to qualified subscribers!

4. If you haven't perused the following web sites recently, they are definitely worth a look. While he's not focused on physical security *per se*, encryption and cyber-security guru Bruce Schneier always has interesting things going on at his web site (<http://www.schneier.com/>). (Bruce is on the JPS Editorial Board.) And Ross Anderson's home page at Cambridge University has a number of intriguing papers you can download that involve physical and electronic security issues (<http://www.cl.cam.ac.uk/~rja14/>).

5. In the Vulnerability Assessment Team at Los Alamos National Laboratory (<http://pearl1.lanl.gov/external/c-adi/seals/index.shtml>), we often work with a number of students ranging from high school students through graduate school. When we first interact with these students, many are very much at home with the idea of conducting research and development (R&D) on cyber security, but quite flabbergasted that there would be many unsolved R&D problems in physical security. What does this say about the future health of the field, and what can be done to change this perspective and attract more interest among young people, especially females and minorities?

6. As vulnerability assessors, we sometimes have a somewhat cynical view of security. This is both inevitable and useful. The following security maxims (or “rules of thumb”) have arisen as a result of 15 years of work on physical security devices, systems, and programs. I would not claim they are absolute laws, but they probably do apply about 90% of the time.

Infinity Maxim: There are an unlimited number of security vulnerabilities, most of which will never be discovered (by the good guys or bad guys).

Arrogance Maxim: The ease of defeating a security device or system is proportional to how confident/arrogant the designer, manufacturer, or user is about it, and to how often they use words like “impossible” or “tamper-proof”.

Ignorance is Bliss Maxim: The confidence that people have in security is inversely proportional to how much they know about it.

High-Tech Maxim: The amount of careful thinking that has gone into a given security device, system, or program is inversely proportional to the amount of high-technology it uses.

Schneier’s Maxim: The more excited people are about a given security technology, the less they understand (1) that technology and (2) their own security problems.

Low-Tech Maxim: Low-tech attacks work (even against high-tech devices and systems).

Yippee Maxim: There are effective, simple, & low-cost countermeasures (at least partial countermeasures) to most security vulnerabilities.

Arg Maxim: But users, manufacturers, managers, and bureaucrats will be reluctant to implement them, often for reasons of inertia, bureaucracy, pride, fear, or wishful thinking.

Bob Knows a Guy Maxim: Most security products and services will be chosen by the end-user based on purchase price plus hype, rumor, innuendo, hearsay, and gossip.

I Just Work Here Maxim: No salesperson, engineer, or executive of a company that sells physical security products or services is prepared to answer a significant question about vulnerabilities, and few potential customers will ever ask them one.

Double Edge Sword Maxim: Within a few months of its availability, new technology helps the bad guys at least as much as it helps the good guys.

Familiarity Maxim: Any security technology becomes more vulnerable to attacks when it becomes more widely used, and when it has been used for a longer period of time.

Antique Maxim: A security device, system, or program is most vulnerable near the end of its life.

Payoff Maxim: The more money that can be made from defeating a technology, the more attacks, attackers, and hackers will appear.

I Hate You Maxim 1: The more a given technology is despised or distrusted, the more attacks, attackers, and hackers will appear.

I Hate You Maxim 2: The more a given technology causes hassles or annoys security personnel, the less effective it will be.

Shannon's (Kerckhoffs') Maxim: The adversaries know and understand the security hardware and strategies being employed.

Corollary to Shannon's Maxim: Thus, "Security by Obscurity", i.e. security based on keeping long-term secrets, is not a good idea.

Gossip Maxim: People and organizations can't keep secrets.

Rohrbach's Maxim: No security device, system, or program will ever be used properly (the way it was designed) all the time.

Rohrbach Was An Optimist Maxim: Few security devices, systems, or programs will ever be used properly.

Insider Risk Maxim: Most organizations will ignore or seriously underestimate the threat from insiders.

Father Knows Best Maxim: The amount that (non-security) senior managers in any organization know about security is inversely proportional to (1) how easy they think security is, and (2) how much they will micro-manage security and invent arbitrary rules.

Huh Maxim: When a (non-security) senior manager, bureaucrat, or government official talks publicly about security, he or she will almost always say something stupid and/or naïve.

Troublemaker Maxim: The probability that a security professional has been marginalized by his or her organization is proportional to his/her skill, creativity, knowledge, competence, and eagerness to provide effective security.

Throw the Bums Out Maxim: An organization that fires high-level security managers when there is a major security incident, or severely disciplines or fires low-level security personnel when there is a minor incident, will never have good security.

7. The *Journal of Physical Security* is primarily meant as a peer-reviewed, scholarly journal for theories, models, commentary, and research and development in the area of physical security. From time to time, however, we will have articles that are not peer-reviewed. This may include reprinted papers that have appeared elsewhere, reviews or viewpoint papers, essays, interviews, and my own editor's comments. You can assume, however, that any research paper that appears in JPS has been reviewed by at least two anonymous, independent reviewers, unless noted otherwise on the first page of the paper in question.

This issue also contains some non-peer-reviewed research papers (papers 2-5) that have come out of my own Los Alamos Vulnerability Assessment Team, and are marked as such. One of the reasons for founding JPS was our frustration at the absence of scholarly, peer-reviewed journals devoted to physical security. Finding a home for these papers elsewhere would probably be a challenge. We could, I suppose, devise some kind of anonymous peer-review process involving the Editorial Board but not the Editors that might resolve some of the conflict of interest in having the Vulnerability Assessment Team (which hosts JPS) publish papers in its own journal, but that is probably not worth the effort. If you find our non-peer reviewed papers just too much vanity self-publishing, feel free to ignore them.

8. As always, comments, suggestions, and complaints are welcome on any topic relevant to JPS. And please consider submitting a manuscript!

9. Thanks for your readership!

10. As always, the views expressed by the editor and authors in JPS are their own and should not necessarily be ascribed to Los Alamos National Laboratory, the United States Department of Energy, or the United States Government.

--Roger Johnston

* Full disclosure: The editor has no financial or other interests in any of the sources or references recommended here. He is, however, grateful to CSO for publishing an interview with him (http://www.csoonline.com/read/060107/fea_qa.html), in addition to placing a version of his (only partially serious) security self-assessment tool on the Internet (http://www2.csoonline.com/quizzes/security_assessment/index.php). He was not compensated for either.